(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－306301

(43)公開日　平成11年(1999)11月５日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｓ
19/07		19/00	Ｎ
19/073			Ｐ

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）

(21)出願番号　特願平10－110924

(22)出願日　平成10年(1998)４月21日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　矢野義博
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

(72)発明者　半田富己男
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

(72)発明者　林　昌弘
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

(74)代理人　弁理士　鞆川　昌信　（外７名）

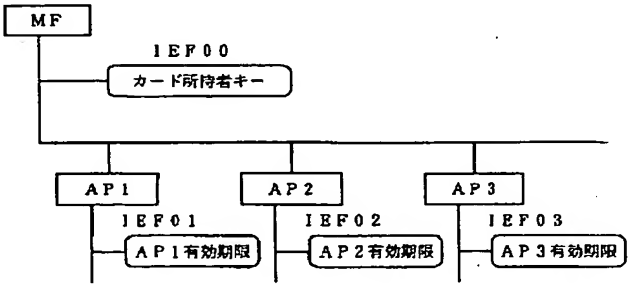
最終頁に続く

(54)【発明の名称】　期限つきセキュリティステータスを有するＩＣカード

(57)【要約】

【課題】　真のカード所持者以外の人物によるＩＣカードの継続的な不正利用を防止する。

【解決手段】　タイマー機能を有するＩＣカードにおいて、カード所持者の認証終了後認証有効状態を示すセキュリティステータスが所定の時間だけ持続するようにしたもので、カード所持者認証の有効期限をマスターキーファイルＩＥＦ００、アプリケーションキーファイルＩＥＦ０１、ＩＥＦ０２、ＩＥＦ０３に設定するようにしたものである。



【特許請求の範囲】

【請求項１】　演算装置、主メモリ、読み出し専用メモリ、不揮発性メモリ、タイマー機能を有するＩＣカードにおいて、カード所持者の認証終了後認証有効状態を示すセキュリティステータスが所定の時間だけ持続するようにしたことを特徴とするＩＣカード。

【請求項２】　上記所定の時間を経過した後、セキュリティステータスを元に戻す、あるいは該当するアプリケーションファイルを閉塞するようにしたことを特徴とするＩＣカード。

【請求項３】　請求項１または２記載のＩＣカードにおいて、カード所持者認証の有効期限をキーファイルに設定したことを特徴とするＩＣカード。

【請求項４】　請求項１または２記載のＩＣカードにおいて、アプリケーションファイル毎にカード所持者認証の有効期限をキーファイルに設定するようにしたことを特徴とするＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は真のカード所持者以外の人によるＩＣカードの継続的な不正利用を防止するようにしたＩＣカードに関する。

【０００２】

【従来の技術】図４に示すように、リーダ／ライタ１はＩＣカード２に対してコマンド（命令）を送信し、これを受信したＩＣカードは、コマンドを解釈して書き込み／読み出し等の処理を実行し、処理結果をレスポンスとしてリーダ／ライタ１へ返すようになっている。

【０００３】図５に示すように、ＩＣカード２は、ＣＰＵ２ａ、ＲＡＭ２ｂ、ＲＯＭ２ｃ、ＥＥＰＲＯＭ２ｄを有しており、ＲＯＭ２ｃに記憶されているプログラムをＣＰＵ２ａに読み込み、リーダ／ライタ１から送信されるコマンドをＩ／Ｏポートを通して受信すると、コマンドとともに送信されたデータを読み込んで必要な処理を行い、結果をＥＥＰＲＯＭ２ｄの所定のファイルエリアに書き込み、Ｉ／Ｏポートを通してレスポンスを出力する。なお、２ｅはタイマーモジュールであり、ＣＰＵ２ａの動作とは独立に動作し、設定された時間が経過すると、ＣＰＵ２ａに対して割り込みをかけて通知する計時装置である。

【０００４】図６はアプリケーションプログラム用領域とオペレーティング・システム（ＯＳ）用領域からなるＥＥＰＲＯＭ３を示したもので、アプリケーション領域の先頭アドレスから、アプリケーションＡ、Ｂ、Ｃのファイルをこの順で割り当てるときに、同時に、ファイルエリアの割当て順に、アプリケーション領域の最後から先頭に向かってＡディレクトリ、Ｂディレクトリ、Ｃディレクトリが形成される。ディレクトリはファイルの制御情報であり、図７に示すように、ファイルを識別するためのファイルＩＤ、ファイルが記憶される先頭アドレス、エリア容量、属性情報（リード／ライトのアクセス権（キー）の情報）、チェックコードからなっている。

【０００５】図６において、アプリケーションの領域に続いたＯＳ用領域には、ディレクトリに示された先頭アドレスとエリア容量から、割り当てられたファイルエリアの最後のアドレスを示すポインタ、積み上げられた最後のディレクトリを示すポインタ等のＯＳが使うデータがセットされる。ポインタＰ、Ｐ′の間の領域がさらに割り当て可能なメモリ領域である。

【０００６】リーダ／ライタからのコマンドは、図８に示すように、コマンドの分類（ＣＬＡ）、命令（ＩＮＳ）、パラメータＰ１、Ｐ２にデータ長Ｌｃおよびデータ部（ファイルＩＤ、エリア容量、属性情報）が付加されたものであり、ファイルの割り当ては、クリエイト・ファイル命令で行われる。

【０００７】

【発明が解決しようとする課題】従来のＩＣカードではカード所持者が端末から入力したキー（ＰＩＮ：Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）をＩＣカード内に格納されたキーと照合し、一致すればセキュリティステータスを更新するようにしたので、それ以降はＩＣカードが非活性化（接続装置からカードが抜かれた状態）されるまではセキュリティ属性が満足されるレベルでファイルへのアクセスが可能であった。

【０００８】図９において、マスターファイル直下のキーファイルＩＥＦ００は、カード所持者キーを表し、ＡＰ１、ＡＰ２、ＡＰ３は専用ファイルＤＦ内のアプリケーションプログラムファイルを示し、ＩＥＦ０１、ＩＥＦ０１、ＩＥＦ０３はそれぞれ各アプリケーションプログラムにアクセスするためのキーＰＩＮ１、ＰＩＮ２、ＰＩＮ３が格納されているキーファイルである。

【０００９】カード所持者の認証（グローバルセキュリティステータス）はＭＦ直下のキーに対するＰＩＮ入力時に行われ、入力されたＰＩＮがＩＥＦ００のキーと一致すると、図１０に示すグローバルステータスが０から１に更新され、それ以降はＩＣカード利用システム側（接続装置側）で明示的にカード所持者の認証手続きを実施しない限り、あるいはＩＣカード側で非活性化されない限り、最初のグローバルセキュリティステータスが保持される。

【００１０】この状態で、各専用ファイルにアクセスするための権限が与えられ、例えばアプリケーションＡＰ１にアクセスする場合は、キーファイルＩＥＦ０１のＰＩＮ１と照合し、これが合致すればＡＰ１にアクセス可能となる。このとき図１０のセキュリティステータスが０から１に更新される。なお、セキュリティステータスは当該アプリケーションファイルにアクセスできる権限であり、他のアプリケーションに対しては及ばない。

【００１１】このように、一旦認証手続きが成功する

と、最初のグローバルセキュリティステータスが保持されるため、カードの真正性の認証手続きをチャレンジ／レスポンスの交換（接続装置とＩＣカード側とで相互に乱数を渡して相手が真正かどうかを確認する手続き）を行ったとしても、接続装置に向かって操作している人物が当初のＰＩＮ入力時に認証した正当なカード所持者から別の不正な操作者に変わっていても検出する手段がなかった。

【００１２】このように接続装置に向かって操作している人物が真正なカード所持者から不正な人物に変わってしまう状況としては、ＰＯＳレジスター端末でのＩＣカードの抜き忘れや携帯電話機にＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｍｏｄｕｌｅ）のＩＣカードを挿入したまま電話機に置き忘れる状況が想定される。

【００１３】本発明は上記課題を解決するためのもので、真のカード所持者以外の人物によるＩＣカードの継続的な不正利用を防止することを目的とする。

【００１４】

【課題を解決するための手段】本発明は、演算装置、主メモリ、読み出し専用メモリ、不揮発性メモリ、タイマー機能を有するＩＣカードにおいて、カード所持者の認証終了後認証有効状態を示すセキュリティステータスが所定の時間だけ持続するようにしたことを特徴とする。また、本発明は、上記所定の時間を経過した後、セキュリティステータスを元に戻す、あるいは該当するアプリケーションファイルを閉塞するようにしたことを特徴とする。また、本発明は、カード所持者認証の有効期限をキーファイルに設定したことを特徴とする。また、本発明は、アプリケーションファイル毎にカード所持者認証の有効期限をキーファイルに設定するようにしたことを特徴とする。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態について説明する。本発明のＩＣカードは図５に示した構成のものと同様であり、タイマー機能を有している。このタイマー機能は外部から供給されたクロックを利用して経過時間を測定し、指定された有効期限の時間が経過したことをＣＰＵ２ａに知らせる機構であり、専用ハードウエァで実現してもソフトウエァによるインターバルタイマーで実現してもかまわない。

【００１６】本発明はセキュリティステータス（認証有効状態）に有効期限を設け、カード所持者のＰＩＮ入力によるカード所持者認証後のセキュリティステータスの有効状態が一定時間だけ継続し、一定時間経過後にセキュリティステータスがカード所持者認証前に戻ることにより、それ以降の継続的な使用はできないようにしたものである。以下で説明する例では有効期限の設定はグローバルセキュリティステータスと各アプリケーションのセキュリティステータスすべてに対して設定しているが、有効期限の設定はこれに限定されるものではなく、例えばグローバルセキュリティステータスのみ、あるいは各アプリケーションのセキュリティステータスに対して、あるいは特定の重要なアプリケーションのセキュリティステータスに対して設定する等適宜行うようにしてもよい。

【００１７】図１に示すように、ＭＦ直下のキーファイルＩＥＦ００、各アプリケーションファイル下のキーファイルＩＥＦ０１、ＩＥＦ０２、ＩＥＦ０３……にはそれぞれ有効期限のレコードが付いている。この有効期限は最初から設定されていても良いし、或いはその後必要性が生じた時に設定するようにしても良い。例えば、認証コマンドでＭＦ直下のキーファイルＩＥＦ００を指定すると、入力されたＰＩＮとファイル内のキーの値を照合後、一致すれば現在のグローバルセキュリティステータスを記憶した後に、グローバルセキュリティステータスを更新すると共に、タイマー機能を開始させる。タイマー機能に対して指示する有効期限は、アプリケーションＡＰ１を利用する場合には、ＩＥＦ００の有効期限（カード全体の有効期限で、例えばあらかじめ設定）とＩＥＦ０１に記録された有効期限の和または差等の四則演算によって求められるようにする。アプリケーションＡＰ２を利用する場合にはＩＥＦ００とＩＥＦ０２のそれぞれに記録された有効期限の和または差等の四則演算によって求められる。また、ＩＥＦ００の有効期限も何らかの演算をして求めるようにしてもよい。このようにしてカード所持者認証の有効期限をアプリケーション毎に可変に設定しておくことができる。もちろん、各有効期限は他のどのような方法によって設定してもよい。

【００１８】図２はカード所持者認証プロセスフローの例を示す図で、左側から右側に向かう矢印は端末側からＩＣカードへのコマンド、右側から左側へ向かう矢印はＩＣカードから端末側へ送られるレスポンスを示している。Ａ１において、カード所持者がアプリケーションを選択し、Ａ２において、ＡＰ１を選択するセレクトファイルコマンド（ファイル選択命令）をＩＣカードに対して送り、正常終了の場合にはＡ３において、ＩＣカード側からステータスワード（９０００）をレスポンスとして返す。次にＶ１においてカード所持者がＰＩＮを端末に入力し、Ｖ２において、認証コマンド（パラメータ＝ＩＥＦ００，ＩＥＦ０１、データ部＝カード所持者が入力したＰＩＮ）が送られ、Ｖ３において、ＩＣカード側ではＰＩＮの照合、タイマーセットを行い、正常終了であればレスポンスとしてステータスワード（９０００）を返す。この状態で、ＡＰ１へのアクセス権が得られ、Ｐ１以降アプリケーションに固有のプロトコルで相互のコマンド／レスポンスが行われる。この間にセキュリティステータス有効期限が経過すると、Ｐｎにおいて、セキュリティステータスを満たさないため、ステータスワード６９８２が返され、カード所持者認証前へ戻ること

になる。そして、さらに継続使用するためには、上記Ｖ１，Ｖ２のプロセスを実行しなければならない。

【００１９】図３は認証コマンド処理の例を示す図で、ＡＰ１へのアクセス権を得る場合の処理フローを示している。認証コマンドでＩＥＦ００とＩＥＦ０１を指定し、ＡＰ１へのアクセスを試みると、まずＩＥＦ００を検索し、ＩＥＦ００が見つかると、現在のセキュリティステータスをメモリ中に記憶し、コマンドのデータ部（カード所持者が入力したＰＩＮの値）とＩＥＦ００のレコード値を照合する（ステップＳ１～Ｓ４）。照合が一致すると、次にＩＥＦ０１を検索し、ＩＥＦ０１が見つかるとセキュリティステータスの有効期限Ｔを算出する（ステップＳ５～Ｓ８）。次いで、タイマー機能を呼出し、引き数Ｔをタイマーに設定（有効期限の設定）する。次いで、レスポンスを編集し（ステップＳ１０）、正常終了のレスポンスを返す（ステップＳ１１）。こうして有効期限が設定されるので、この期限を経過するとセキュリティステータスを満たさなくなり、継続使用の場合には再度認証処理を行わなければならない。なお、ステップＳ５において、ＩＥＦ００の照合が失敗した場合には、ステップＳ１０に飛んでレスポンス内容を編集し、エラーを返す。

【００２０】

【発明の効果】以上のように本発明によれば、真正なＩＣカード所持者によるＰＩＮ入力認証後にＩＣカードを挿入した端末装置が不正な利用者の手に渡った場合でも、不正利用者によるＩＣカードの継続的な利用を阻止することができる。ＩＣカードを利用したシステムで特にカード所持者の認証を厳密に行わなければならないシステム、例えば電子現金システムにおいて、本発明のＩＣカードを利用することにより、ＩＣカード自体が定期的にセキュリティステータスをカード所持者のＰＩＮによる照合認証前の状態に戻してしまうので、仮に不正利用者の手に渡ったとしても重要な現金情報ファイルのセキュリティ属性を満足できなくなり、継続的な不正利用を阻止することができる。

【図面の簡単な説明】

【図１】　本発明のファイル構造を説明する図である。

【図２】　カード所持者認証プロセスフローの例を示す図である。

【図３】　認証コマンド処理の例を示す図である。

【図４】　リーダ／ライタとＩＣカードの通信を説明する図である。

【図５】　ＩＣカードの構成を説明する図である。

【図６】　ＥＥＰＲＯＭの構成を説明する図である。

【図７】　ディレクトリの構成を説明する図である。

【図８】　コマンドの構成を説明する図である。

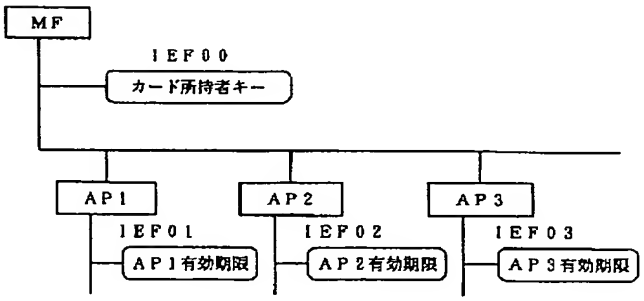
【図９】　ファイル構造を示す図である。

【図１０】　セキュリティステータスを説明する図である。

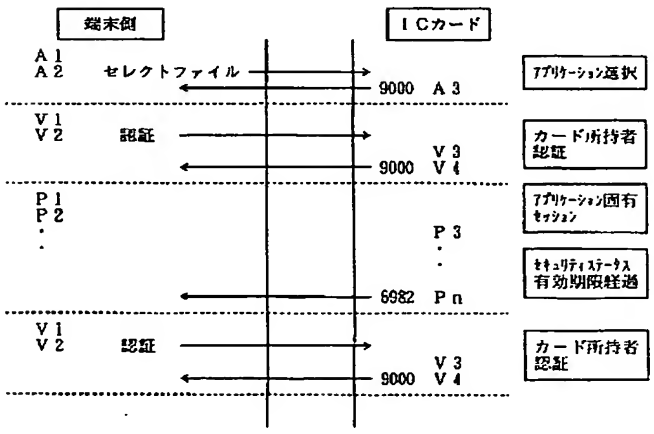
【符号の説明】

１…リーダ／ライタ、２…ＩＣカード、２ａ…ＣＰＵ、２ａ…ＲＡＭ、２ｂ…ＲＯＭ、２ｄ…ＥＥＰＲＯＭ、２ｅ…タイマー。

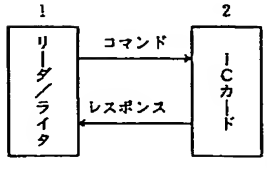
【図１】



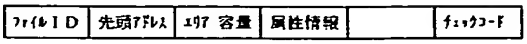
【図２】



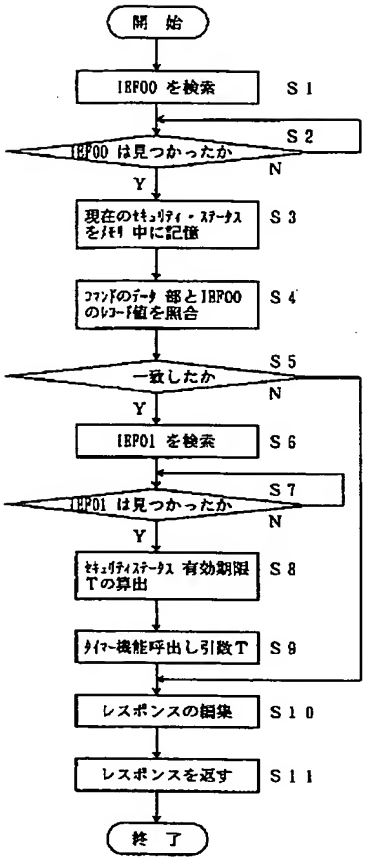
【図４】



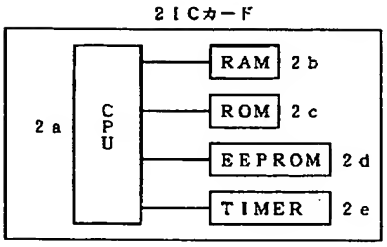
【図７】



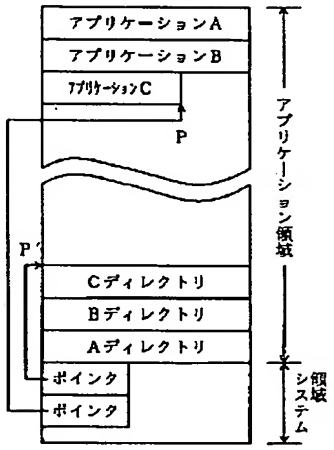
【図３】



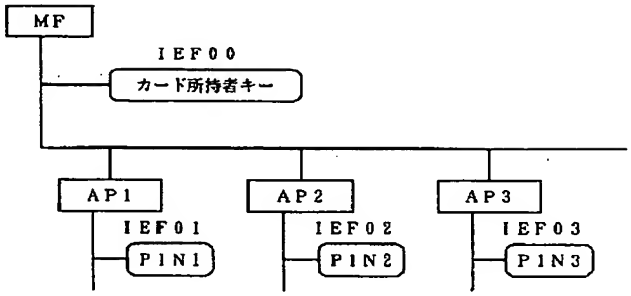
【図５】



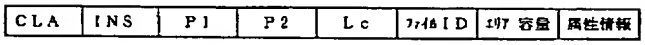
【図６】



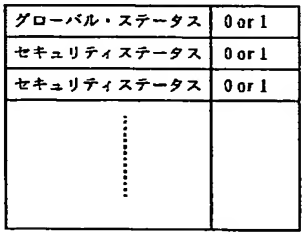
【図９】



【図８】



【図１０】



フロントページの続き

(72)発明者　牧野　寛
山形県山形市松波一丁目１番１号大日本山形アイ・エス・ディー株式会社内